017.40746X00
28565

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: **Koskimies OSKARI**

Invention: **WIRELESS LOCK SYSTEM**

Prepared by:

Antonelli, Terry, Stout & Kraus, LLP
1300 North Seventeenth Street. Suite 1800
Arlington, Virginia 22209
Tel: 703/312-6600
Fax: 703/312-6666

TITLE: WIRELESS LOCK SYSTEM

Background of the Invention:

Field of Invention

The invention relates generally to a wireless lock and key system and more particularly to controlling and managing an electronic lock, key and control device, and to creating easily distributable temporary keys to said locks.

Description of the Prior Art

Current locks are all based on the principle of a shared secret between the lock and the key. There are four main lock types, and each has its problems:

1) Mechanical locks, where the secret is the way the key is formed.

- The user has to carry a separate key for each lock he can access. The keys have to be dug out of handbag or pocket every time a door is opened.
- Distribution of keys is cumbersome and has to be done by hand.
- Creating keys requires special equipment.
- Invalidating keys is hard.
- The use of keys cannot easily be limited (e.g. to office hours).

2) Electronic locks with (possibly wireless) keys, where the secret is an access code stored in both lock and key.

- While a key may have space for several codes, this is uncommon and the number of codes is limited. Thus, the user still has to carry many keys, especially as the systems are incompatible with each other. Note that if the same code is used in all locks, then the owner of any lock is able to create a key for opening all the other

locks. Thus, you would have to trust the owners of all locks that you use.

- Distribution of keys is cumbersome and has to be done by hand.
- Creating new keys usually requires special equipment, and even if a key can store several codes, access to the lock is required. While access to the lock is not necessary if a single, known code for the lock is always used, this would also mean that all the created keys share the same code and cannot be separately controlled. For instance, it would not be possible to revoke just a single key.

3) Keyless mechanical or electronic locks, where the user has to remember the code and enter it whenever access is needed.

- While the user does not have to carry keys, he has to remember all his codes, which is actually worse for many people.
- Creating new keys (codes) requires access to the lock.
- While codes can be distributed electronically, they can be used by anyone, making use of secure channels necessary.
- The code can be learned by secretly observing the user as he enters the code.

4) Keyless electronic locks, where the user's fingerprint, retinal scan or other similar feature is used for identification.

- The required scanning devices are expensive.
- Creating new "keys" requires access to the lock.

- In theory, if your information is stored on a lock, the owner of that lock can use that information to e.g. create a replica of your finger for opening all locks you have